Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SE05/000230

International filing date: 18 February 2005 (18.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/545,870
Filing date: 19 February 2004 (19.02.2004)

Date of receipt at the International Bureau: 22 April 2005 (22.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 08, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/545,870*
FILING DATE: *February 19, 2004*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

L. Edelen

L. EDELEN
Certifying Officer

PTO/SB/16 (10-01)
Approved for use through10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. ER054906291US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Jakob	Ehrensvärd	Täby, Sweden

□ *Additional inventors are being named on the _______ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

SECURE DATA MANAGEMENT DEVICE AND METHOD

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

□ Customer Number ____________ → *Place Customer Number Bar Code Label here*
Type Customer Number here

OR

☑ Firm *or* Individual Name	Don W. Bulson, Esq.				
Address	Renner, Otto, Boisselle & Sklar, LLP				
Address	1621 Euclid Ave., 19th Fl.				
City	Cleveland	State	Ohio	ZIP	44115
Country	United States	Telephone	216-621-1113	Fax	216-621-6165

ENCLOSED APPLICATION PARTS ***(check all that apply)***

☑ Specification *Number of Pages* 9
□ Drawing(s) *Number of Sheets* ____
□ Application Data Sheet. See 37 CFR 1.76
□ CD(s), Number ____
☑ Other (specify) Return Postcard

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

□ Applicant claims small entity status. See 37 CFR 1.27.
☑ A check or money order is enclosed to cover the filing fees
□ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: ____________
□ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) $180.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.
☑ No.
□ Yes, the name of the U.S. Government agency and the Government contract number are: ____________

Respectfully submitted,

SIGNATURE Don W Bulson

Date 02/19/2004

TYPED or PRINTED NAME Don W. Bulson

REGISTRATION NO. *(if appropriate)* 28,192

Docket Number: STOCP0135US

TELEPHONE 216-621-1113

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Secure data management device and method

Recent developments in microelectronics have enabled integration of microprocessor-based systems into typical low cost, disposable items. However, little or no attention has been to address basic data security matters.

Embedding an electronic data collection device into a packaging enables the packaging to become "intelligent", and allows it to collect information about its usage and its environment.

A typical application is a pharmaceutical packaging with integrated electronics, as described in patent US 6,244,462. The packaging is capable of registering when each dose was removed from the device. Together with means of communication, the packaging can exchange data with a host computer system. By adding additional features, such as an electronic questionnaire as described in patent US 6,628,199, additional data can be collected and time-stamped at point of use.

However, in most applications, several concerns arise in terms of data security. If considering an application where patient data is stored in a packaging as described above, sensitive information must be exchanged with a host system. The growth of the Internet has made it attractive to remotely update and retrieve information from a large number of devices, potentially scattered over a large geographical area. The typical security issues addressed are:

Identity authentication

To identify a unique item from a host system, each item needs to hold a unique identity. In order to prove the identity, a form of authentication scheme is required to prevent counterfeiting and other identity fraud mechanisms.

Confidentiality

Transmitting information over public networks always involves the risk of eavesdropping. In order to prevent transmitted information from being used by unauthorized, the information needs to be encrypted.

Authenticity

Information being transmitted is vulnerable to different forms of fraudulent modification. By adding a cryptographic checksum, involving a cryptographic operation, a "watermark" is created, which can be used to detect any illegal modification of the data.

Non-repudiation and proofing

A more specialized form of authentication involves proofing, where a piece of information needs a digital signature, which can be verified. In order to assure that only the creator of the information should be able to create the signature, but potentially a large number of receivers should be able to verify it. In order to enforce non-repudiation, asymmetric encryption schemes are typically used.

Although the above described security issues can be handled by a client computer, retrieving information from the device, that scheme adds some concerns:

Key distribution
Distributing encryption keys to a wide number of users is a major undertaking and possesses threats of keys being compromised. Further, invalid keys used by end-users typically render received information unusable.

Key management
Key management strategies to maintain key integrity in a remote environment are often not practically feasible to enforce. The risk of an unintended or indented (fraud) key compromise would render the security of the system worthless.

Non-repudiation
Considering non-repudiation schemes involving digital signatures requires a very tight control over the private key. The user in possession of a private key may use the private key outside its scope, thereby making the digital signatures worthless.

The conclusion is that key distribution and management in a distributed system is difficult to implement, considering risks of malfunction and key compromise.

In summary, a device and method to address the data security issues described above would enable a wider usage and acceptance of intelligent devices and packaging.

Description of the preferred embodiment

The present invention describes a product packaging with integrated microelectronics and a method to securely exchange information between said device and a host computer over a public network. The present invention does not make a general scope by addressing all settings involving a "device" and a "host computer", but rather the specialized scope, where a data storage and collection device is embedded into a product enclosing, i.e. packaging material, envelope, container, etc.

In detail, the preferred embodiment describes an enhancement of a single-use pharmaceutical packaging with an integrated electronic module (EM), known as a combination of patents US 6,244,462, and US 6,628,199. The basic purpose of the microelectronics is to monitor the state of a plurality of printed circuit lines printed onto the packaging material. A change in the resistive properties of a circuit line, signals a possible event that is processed by the EM, where a stable detected event is typically stored in a non-volatile means, together with a time-stamp. A contact-less communication transceiver embedded in the packaging material is used to exchange information with a host computer system. An example of a suitable implementation of a communication interface is described in patent US 6,615,023.

The novelty of the preferred embodiment states a security approach which is made as an integral part of a product itself, and describes necessary enhancements needed to ensure a range of data security issues, when exchanging data between the packaging and a host computer system over an insecure communication channel.

The functionality of the EM is extended to include a cryptographic processor and storage for at least one cryptographic key. The basic requirement of the cryptographic processor is to perform encryption and decryption, using a symmetric algorithm, such as DES, 3DES, AES or equivalent. In order to fully support digital signatures in a Public Key Infrastructure (PKI) environment, the cryptographic processor must also support an asymmetric algorithm, such as RSA.

The nature of the EM key storage must be storage only, i.e. the key can be written to the EM, but not retrieved. The key is then only used in cryptographic operations and is securely stored in the secured storage of the EM. Cryptographic keys should preferably be entered in a secure environment where there is no risk of eavesdropping or key in other ways get compromised.

Further, the EM also features storage for an address to a host computer in a computer network, having the ability to exchange data with the device in a secure manner.

Still further, each EM is factory-programmed to include a unique identity. Although not extremely critical from a security viewpoint, the uniqueness of the identity should be maintained.

Below is a basic scheme to securely exchange information between a host computer (Host) in a computer network (Network), and an intelligent packaging (Device). In reality, the intelligent packaging cannot be directly connected to the computer network. This typically occurs through a network-connected terminal, further featuring an interface to exchange data with the intelligent packaging (Reader). In order to simplify the description from a conceptual viewpoint, the details of the "proxy terminal" and interface is omitted in the following text.

1. The device is placed on the reader
2. The device holds an address, typically a Universal Resource Locator (URL) of the host computer. Said URL is used to automatically establish a connection to the host in the computer network.
3. The device transmits its unique identity to the host in clear text. The host performs a search in a database to get the appropriate cryptographic key, used for secure operations with said device.
4. The host issues a random number, which is transmitted to the device as a challenge
5. The device encrypts the challenge, together with its unique identity and sends back the result as a response.
6. The host decrypts the received response and verifies that the result matches the issued challenge and the initial received identity. If the entities match, the device is considered to be authentic.
7. The host requests data from the device, and initiates Chained Block Cipher (CBC) encryption by sending an Initialization Vector (IV). The initialisation vector prevents attempts to replay previously transmitted data
8. The device transmits data to the host, encrypted in CBC mode.
9. The first transmitted block includes a linear counter and a time reference, if applicable, to make two subsequent transmissions for the same data guaranteed different, thereby thwarting attacks involving comparing data.
10. The final block should be a known signature, such as the device identity padded with zeroes, allowing the host to detect that all data has been received successfully
11. The host receives the data en decrypts it. The signature in the last block is verified to ensure that the received data was authentically received and without errors.
12. The host performs necessary operations on the data and returns a suitable completion message to the device

Depending on security policy, step 4-6 may be considered obsolete and therefore be omitted, if steps 9-10 is implemented correctly.

In order to rely on established infrastructure and allow compatibility with typical corporate firewalls, all data may be passed with the HTTP protocol, through a web-browser on the device side and a web-server on the host side. Received data would then typically be stored in hidden fields in a normal HTML form. An additional benefit of passing the data through a web browser is the simplicity and elegance from the user's point of view:

1. The user puts the device on the reader

2. The web browser is automatically launched and the user is informed that data is being transferred
3. When data transfer is complete, the web server issues a completion screen, typically giving a summary of the data received. An additional audible message may be included in the completion HTML form to notify the user that the transfer was successful.
4. The user removes the device from the reader.
5. The browser is closed automatically

Considering an automated scheme like this, interactive products can be supported in a very simple way. Depending on the automated evaluation of the data received, different screens may be presented to the user, such as "There is only one dose left in your packaging. Would you like to order a new one now?" or "The regimen has not been followed properly. Please contact your physician now".

In order to implement a "zero knowledge protocol", i.e. avoiding to reveal any information at all, a mutual challenge protocol extension can be implemented as:

1. The unique device identity is not transmitted as clear-text. Instead, the identity is concatenated with a random number and then encrypted with a second-level key, shared with all devices in a given group.
2. A host having a shared key with the device group, will be able to successfully decrypt the data from the device and hereby get the device identity.
3. In order to get more data from the device, the host responds with the decrypted data, where one bit in the challenge has been inverted. The result is again encrypted and passed to the device.
4. The device opens for further communication if the decrypted received data matches the random number issued in step 1, corrected for the inverted bit of step 3.

Another aspect of the invention, not previously described, is to use the cryptographic processor to generate digital signatures for data, allowing third-party verification of the data received. In some applications, where the complexity and processing intensive nature of asymmetric signature generations is not feasible, different forms of arbitrated schemes, using less complex symmetric encryption, may be applied.

Public Key Infrastructure (PKI) scheme:
Using asymmetric encryption allows generation of qualified digital signatures, with different keys for signature generation and verification. The keys are generally known as "private" for signature generation and "public" for signature verification. The private key is stored in a tamper resistant device and cannot be read-out. The public key is given to all parties involved in verifying the signatures created by the private key.

A typical scheme may look like:

1. A second level key storage is used in the EM. The first key storage is used for decryption of data in the transmission only.

2. An asymmetric key pair is generated. The private key is programmed into the EM as a second key, and should then be discarded. The public key deployed to the party/parties responsible for verification of data.
3. Following the basic scheme described above, an additional signature is generated by the EM using the private key, operating on a condensed part of the information being transmitted. The signature is transmitted to the host
4. The host validates the received asymmetric signature using the public key. The signature may be stored for future reference if there is a dispute over the validity of the data.

It is important to understand the implication of having two different keys stored in the EM, one for confidentiality (and potentially for integrity) and one for creating a legally viable signature.

By including a time reference generated by the EM at time of information retrieval further enables resolution in non-repudiation matters, as each data transmission then implicitly contains a digitally signed time reference.

For applications where asymmetric encryption is not feasible, an arbitrated scheme can be implemented as:

1. A second level key storage is used in the EM. The first key storage is used for decryption of data in the transmission only.
2. A trusted party generates and stores a symmetric key in said key storage.
3. A copy of the key is kept in a secure storage, accessed by the trusted party only.
4. When data is transmitted to the host, the EM performs a symmetric encryption on the final block, using the arbitrator's key
5. The host keeps the arbitrated signature for further reference in case of a dispute. The arbitrator will then verify the authenticity of the signature using its copy of the symmetric key.

Yet another implementation relying on symmetric encryption could be implemented as:

1. A trusted party generates a symmetric key
2. The key is stored in the key storage of the EM. The EM is programmed to be able to perform encryption only, using said key
3. The trusted party stores a copy of the symmetric key in a tamper resistant device, such as a Smart Card or similar, programmed to allow decryption of data only
4. When data is transmitted to the host, all data is streamed through the tamper resistant device, which returns information in clear text
5. The host verifies that the received signature is authentic and relies on the fact that only the EM can encrypt the information.
6. The arbitrator may not be necessary (and may therefore discard the symmetric key after it has been programmed into the EM and the tamper resistant device), as the host can verify the authenticity of received transaction. However, if the [non rep]

All the protocols described above are described in one direction. From a conceptual viewpoint, the protocols are symmetric, i.e. information transmitted from the host to the device can be secured in the same fashion.

In summary, the device and method implementation details described in the present invention serves the purpose of ensuring several aspects of information security. By storing cryptographic keys in the device itself, both the key distribution and management is solved in a straight-forward manner.

It should be obvious to anyone skilled in the art, that the present invention is not limited to usage with pharmaceutical packaging. As one example, another application with similar constraints would be an intelligent courier packaging. Such an application would physically monitor the shipment for damages and unintentional openings and potentially monitor environmental parameters, such as temperature, shock and air pressure. All information exchanged with the packaging will then be secured by the methods described above.

What is claimed is:

1. A data collection device for communication with a host computer through data network having sensor means, time-keeping means, non-volatile memory means, a device unique identity code, data processing means, cryptographic processing means and data communication means, characterized by said data collection device being integrated as an integral part of a container of a product, said data collection device retrieving information about said product's usage and environment, said information being stored in said non-volatile memory means, said cryptographic processing means performing at least one cryptographic operation on information being exchanged between the device and a host computer system.

2. A device in accordance with claim 1, characterized by said non-volatile memory means is further used to store an address reference to said host computer to allow automatic connection to said host computer through said computer network.

3. A device in accordance with claim 1, characterized by said time-keeping means being used to generate a timestamp, said timestamp being stored together with information retrieved by said sensor means

4. A device in accordance with claim 1, characterized in said cryptographic operation involve symmetric encryption, symmetric decryption, asymmetric encryption, asymmetric decryption, key generation, message digest or any combination thereof.

5. A device in accordance with claim 1, characterized by said non-volatile storage means is further used to store at least one cryptographic key, said key being used as an operator in said cryptographic operation.

6. A device in accordance with claim 5, characterized by the contents of said information storage means can be exchanged with said host computer, exclusive said encryption keys.

7. A device in accordance with claim 6, characterized by said cryptographic operation performing encryption of data stored in said memory means prior to transmission using said data communication means

8. A device in accordance with claim 6, characterized by said cryptographic operation performing decryption of data received through said communication means prior to storage in said memory means

9. A device in accordance with claim 1, characterized by said cryptographic operation being applied on an arbitrary data string received by a host computer concatenated with said unique device identity

10. A device in accordance with claims 7 and 8, characterized by said exchanged information being cryptographically processed block-wise in Chaining Block

Cipher (CBC) mode, where the first block transmitted having a time variant property

11. A device in accordance with claim 10, characterized by the last block in said transmitted information contains a known signature, which can be validated by the receiver to verify that all transmitted data has been received correctly.

12. A device and host computer in accordance with claim 6, characterized by the host computer having a stored cryptographic key being different from the cryptographic key stored in the device

13. A device and host computer in accordance with claim 12, characterized by the device having encryption capabilities for a given device key only and the host computer decryption capabilities for a given host key only

14. A device and host computer in accordance with claim 12, characterized by the device having decryption capabilities for a given device key only and the host computer encryption capabilities for a given host key only